REMARKS

Claims 49-87 remain in this application, with Claims 1-48 previously cancelled, Claims 49-79 amended, and new Claims 80-87 added. Applicants respectfully request review and reconsideration of the application in view of the foregoing amendments and following remarks.

At the outset, Applicants acknowledge with appreciation the withdrawal of the previous grounds of rejection. As will be further addressed below, Applicants consider all pending claims in the application to be allowable over the prior art of record.

The Examiner objected to Claims 73-75 for improper dependency. Applicants have amended Claim 73 to correct this error. Also, the Examiner rejected Claims 49-69 under 35 U.S.C. § 112, second paragraph, as indefinite due to the use of the abbreviation ID. As will be further discussed below, Applicants have amended each of the pending claims to replace the abbreviation with more precise terms, e.g., "state identifier." This ground of rejection should therefore be withdrawn.

Before addressing the merits of the latest rejections based on prior art, Applicants provide the following brief description of the invention. The present invention is directed to a novel approach for allowing a client to maintain state with a web application operating on a remote server while protecting the user's security and privacy. Most web applications are "stateless" applications insofar as the server has no way of knowing whether a series of requests are coming from the same client and pertaining to the same transaction. Thus, the server will deliver web pages in response to page requests without knowing whether these deliveries are part of the same user session. In order to maintain state, i.e., to group together communications that are part of the same user session, the server may generate a unique sessionID, which the server then communicates and stores on the client in the form of a cookie. The client would then include that identifying sessionID with each subsequent communication, and thus allow the server to associate different web page requests as part of the same user

session. For example, a shopping cart application of a retailing website would use a cookie to track a client as it moves from page-to-page through the website and recognize the movements as part of a common user session.

A drawback of this approach is that it creates a security problem from the users' perspective in that their computer must be "open" to permit the server applications to store information on the computer. Many computer users do not want web application servers to store files on their computers due to concerns over receiving illicit code such as viruses that can infect their computers or so-called "spyware" that monitors clients behavior on the web. As a result, many computer users selectively configure their browsers to block cookies from being stored onto their computer, thereby also preventing web applications from maintaining state with the clients.

The present invention provides a solution that enables the web applications to maintain state with the client while at the same time preventing the web application from storing files onto the computer. According to an embodiment of the invention, the client generates a unique state variable at its end (referred to as a "state identifier" in the amended claims), and then communicates the state variable to the server for use in associating different web page requests as part of the same user session. This has great benefit, since web browser applications no longer need to be "open" in the sense that web servers no longer need to store information on the client machines to maintain state with the client. The client may selectively transmit the state variable to the server as an http header with each uniform resource locator ("URL") request. The server receiving these requests compares the state variable to information stored in a database to determine if the user has a current transaction status that should be taken into account in the server's response.

More particularly, the unique state variable (or state identifier) may be based on location data corresponding to the geographic location of the client and/or temporal data corresponding to the time at which the user invoked the current Internet browser session. The location and/or temporal data serves as a proxy for identifying the client,

since in most cases only a single computer would satisfy the location and/or temporal parameters, while at the same time not disclosing to the server other more sensitive identifying information (such as user name or password). The client may reformat these values into character strings of known lengths and then concatenate them together into a single character string to generate the state identifier. To make the state identifier anonymous, the client may mathematically encode the characters of the state variable. When the user terminates the current browser session, the client may delete the state variable, thereby blocking the remote server's ability to monitor the user's activity in future transactions. Thus, the remote server is able to provide the user with more functionality than it otherwise would be able to offer operating in a stateless protocol, while the client can maintain enhanced security over the conventional use of cookies that allow the server to continuously monitor client behavior.

Applicants have amended the claims to clarify these and other aspects of the invention. In particular, Applicants have replaced the term "user ID" with "state identifier," which is deemed to more accurately reflect the invention to the extent that the variable is intended to identify state without giving away other sensitive information with which to identify the particular client. Applicants consider the amended claims to be in condition for allowance, as further discussed below.

The Examiner rejected Claims 49-52, 56-61, 65, 66, 68-72 and 76-79 under 35 U.S.C. § 103(a) as unpatentable over Dustan et al. in view of MacDoran et al. Applicants respectfully traverse these rejections.

Dustan et al. discloses a method for accessing information that is consistent with the above description of the prior art. In particular, a client accesses a network server by requesting a logon menu. A logon input is then communicated to the network server, which in turn communicates the logon input to a database server. The database server verifies the logon input and generates a unique session identification number, which is communicated to the client for storage on the client computer. In subsequent communications with the server, the client provides the session identification number,

enabling the server to verify that the session identification number and logon input are valid.

The Examiner refers to the communication by the client of the account number and password as providing the "state identifier" described in the patent application (citing to Dustan et al., Fig. 5, reference number 176). The account number and password are validated to determine whether to permit client access to the network. See col. 17, lns. 58-67. But, it should be appreciated that the account number and password are not used by the server to maintain state, i.e., to determine whether a particular communication is part of a common user session. Instead, the server generates a session ID for the purpose of maintaining state and provides that information back to the client. See Fig. 5, reference numbers 212, 216.

Hence, Dustan et al. discloses the conventional use of cookies that are generated at the server end and communicated to the client for storage on the client. This conventional state-identifying method causes the significant security concerns discussed above, and that are overcome through the use of the present invention. Dustan et al. fails to suggest or disclose a system in which a session ID (or other state variable) is generated by the client and communicated to the server to maintain state.

The Examiner acknowledges that Dustan et al. does not disclose the use of location information in the generation of an identifier, and proposes the combination with MacDoran et al. MacDoran et al. discloses a method for authenticating the identity of a remote user through the use of information specific to the location of the user. This teaching is of little applicability to the present invention to the extent that the invention is directed to maintaining state between client and server, and not to authentication of the client. MacDoran et al. does not disclose any use of location information as a state variable, and hence fails to make up for the deficiency of Dustan et al. Moreover, there is no teaching or suggestion to use the location information of MacDoran et al. in the method of Dustan et al.

With respect to Claim 49, the proposed combination of references fails to

suggest or disclose the steps of:

generating a unique state identifier that contains information based on a location value of the client;

transmitting said state identifier from the client to said server in an initial communication with said server;

storing said state identifier in said database in association with a record of a first user session with the client;

transmitting said state identifier to said server in a subsequent communication with said server; and

determining whether the subsequent communication is part of the first user session by comparing the subsequently transmitted state identifier with the initially transmitted state identifier stored in the database, and if there is a match, then associating said second communication with said record of the first user session.

As discussed above, Dustan et al. fails to disclose a "state identifier" that is generated by the client, and communicated to the server in an "initial communication with said server." Dustan et al. further fails to disclose such a client-generated "state identifier" that enables the server to determine whether a "subsequent communication" should be associated with a "first user session." Moreover, Dustan et al. fails to disclose the use of location information in a "state identifier" and there is no teaching or suggestion to combine Dustan et al. with MacDoran et al. Even if combined as proposed, the combination of references fail to suggest or disclose all limitations of the claim.

With respect to Claim 58, the proposed combination of references fails to suggest or disclose a server in communication with a database and adapted to:

receive an initial communication from said client that includes a unique state identifier, said state identifier being derived from location data corresponding to said client;

store said state identifier in said database as a state variable associated with a user session with the client;

receive a subsequent communication from said client that includes a state identifier; and

access the database to determine whether said subsequent communication is associated with said first user session by comparing the subsequently received state identifier with the initially stored state identifier.

As discussed above, Dustan et al. fails to disclose a "state identifier" that is communicated to the server in an "initial communication" with the client. Dustan et al. further fails to disclose such a "state identifier" that is stored by the server as a "state variable" that enables the server to determine whether a "subsequent communication" should be associated with a "first user session." Moreover, Dustan et al. fails to disclose the use of location information in a "state identifier" and there is no teaching or suggestion to combine Dustan et al. with MacDoran et al. Even if combined as proposed, the combination of references fail to suggest or disclose all limitations of the claim.

With respect to Claim 66, the proposed combination of references fails to suggest or disclose a processor in communication with a GPS receiver and adapted to:

generate a state identifier from said location data in association with a first user session between said user and said web application;

transmit the state identifier to the server during the first user session;

store said state identifier in said memory;

transmit a request to said server and include said state identifier in said request if said request is part of said first user session; and

alternatively, generate a new state identifier and include said new state identifier in said request if said request is part of a new user session.

As discussed above, Dustan et al. fails to disclose a "state identifier" that is generated at the client side and transmitted to the server "during the first user session." Dustan et al.

further fails to disclose the generation of a "new state identifier" if a subsequent request is part of a "new user session." Moreover, Dustan et al. fails to disclose the use of location information in a "state identifier" and there is no teaching or suggestion to combine Dustan et al. with MacDoran et al. Even if combined as proposed, the combination of references fail to suggest or disclose all limitations of the claim.

With respect to Claim 70, the proposed combination of references fails to suggest or disclose a method for communicating between a client and a server comprising:

> generating a state identifier based on at least location data that corresponds to a location of said client;
>
> incorporating said state identifier into a communication;
>
> sending said communication to said server;
>
> comparing said state identifier to information stored in a database, said database being in communication with and accessible by said server;
>
> identifying said communication as part of a previous session if there is coincidence between said state identifier and information stored in said database; and
>
> identifying said communication as part of a new session if there is no coincidence between said state identifier and information stored in said database.

As discussed above, Dustan et al. fails to disclose a "state identifier" that is communicated to the server and that enables the server to determine whether a "communication" is part of a previous session or a new session. Moreover, Dustan et al. fails to disclose the use of location information in a "state identifier" and there is no teaching or suggestion to combine Dustan et al. with MacDoran et al. Even if combined as proposed, the combination of references fail to suggest or disclose all limitations of the claim.

For each of the above reasons, this ground of rejection should be withdrawn.

The Examiner further rejected Claims 53-55, 62-64, and 73-75 under 35 U.S.C. § 103(a) as unpatentable over Dustan et al. in view of MacDoran et al., and further in view of Fraker et al. Fraker discloses an apparatus for logging position and time-at-position data in accordance with time and position data broadcast by a number of earth orbiting satellites. The Examiner cites Fraker merely for its disclosure of temporal data. Fraker otherwise fails to suggest or disclose anything relating to maintaining state between client and server, and specifically fails to suggest or disclose the desirability of using temporal data in a state variable. There is no teaching or suggestion for the proposed combination. This ground of rejection should be withdrawn.

The Examiner further rejected Claim 67 under 35 U.S.C. § 103(a) as unpatentable over Dustan et al. in view of MacDoran et al., and further in view of Hunter. Hunter discloses a JAVA function that causes cookies to expire when the browser exits (see public void Cookie.setMaxAge). Notably, this attribute is defined by the creator of the cookie, i.e., the server, and hence the client cannot control the expiration of the cookie. In the present invention, the client creates and deletes the state identifier, providing direct control over the security of the communications. Hunter fails to suggest or disclose a method for maintaining state between client and server in which the client generates the state identifier and can also delete the state variable upon termination of the browser session. This ground of rejection should also be withdrawn.

New Claims 80-87 are directed to an embodiment of the invention in which a method for communicating between a client and server includes:

> initiating a user session with the server by communicating from the client to the server an initial request message over a stateless network protocol, the initial request message further including a unique, client-generated state identifier, the server creating a record in the database associated with the user session with the state identifier contained therein;
>
> conducting the user session in which the server provides at least one

response to the initial request message, and in which any subsequent request messages communicated from the client to the server include the same state identifier, the server associating the initial request message and the subsequent request messages together as part of the user session by verifying correspondence with the state identifier contained in the database record; and

ending the user session by discontinuing communication of further request messages from the client to the server and deleting the state identifier from the client.

The prior art of record fails to suggest or disclose these aspects of the invention for the reasons set forth above. Support for the newly added claims may be found in the specification generally, and in particular at page 6, lines 18-22; page 15, lines 13-17; and, page 16, lines 13-17.

In view of the foregoing, the Applicants respectfully submit that Claims 49-87 are in condition for allowance. Reconsideration and withdrawal of the rejections is respectfully requested, and a timely Notice of Allowability is solicited. If it would be helpful to placing this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

To the extent necessary, Applicants petition the Commissioner for a one-month extension of time, extending to February 12, 2006, the period for response to the Office Action dated October 12, 2005. A check in the amount of $60.00 is enclosed for the one-month extension of time pursuant to 37 CFR §1.17(a)(1). The Commissioner is authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,

Date: February 6, 2006

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000